Georgia Tech Research Institute

Trusting Smart Cities: Risk Factors and Implications

Margaret L. Loper, Ph.D.

Chief Scientist, Information & Communications Lab

margaret.loper@gtri.gatech.edu

September 6, 2019

"Trusting Smart Cities: Risk Factors and Implications," Small Wars Journal, presented at the TRADOC Mad Scientist Conference on Installations of the Future, June 19, 2018

Proclamation

United States Army Training and Doctrine Command

Deputy Chief of Staff, Intelligence

Mad Scientist

Whereas, The Mad Scientist Initiative encourages continuous dialogue and collaboration among academia, industry, government, and non-traditional partners;

And Whereas, The Mad Scientist Initiative identifies tomorrow's key innovations today so the U.S. Army is successful in the future operational environment;

And Whereas, The Mad Scientist Initiative supports Army Learning and Capability development;

And Whereas, Dr. Margaret Loper has provided great and valuable insights and contributions to furthering the mission, goals, and understanding of the Mad Scientist Initiative.

Now, Therefore, by virtue of the authority vested in me as the TRADOC Deputy Chief of Staff, Intelligence, I do hereby proclaim that

Dr. Margaret Loper

be known henceforth and forevermore as an official Mad Scientist, with all the rights and privileges pertaining thereto. May you always seek the future boldly, actively question conventional wisdom and assumptions, and passionately challenge the status quo.

In Witness Whereof, I hereunto set my hand this 19th day of June 2018.

Mad Scientist Initiative

Thomas F Greco

THOMAS F. GRECO
Defense Intelligence Senior Executive
Deputy Chief of Staff, G-2

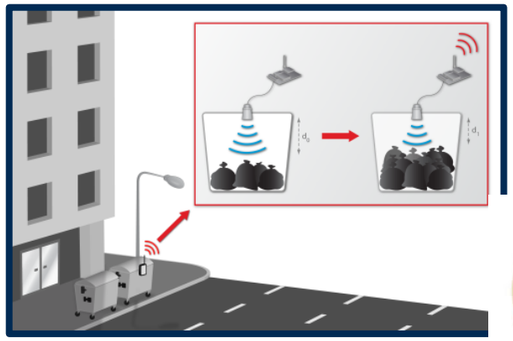
Rise of Smart Cities

Surrounded by billions of sensors, devices and machines

Improve quality of life, efficiency of urban operation and services, and competitiveness

**The idea of a smart city can be applied to smart military installations, smart compounds, and smart campuses

Commercial Smart City Technologies



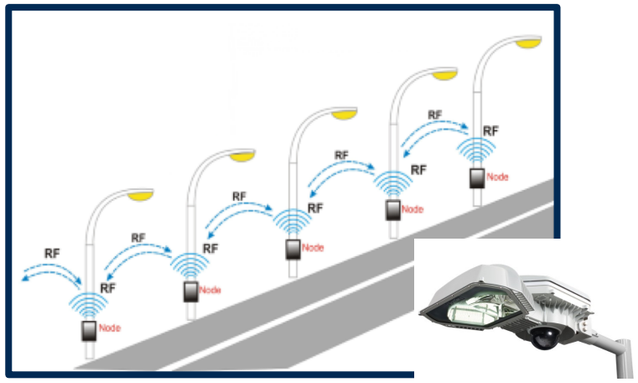

Smart Waste Collection

Security: Video, License Plate Recognition, Gunshot Detection

Efficient Buildings

Transportation: Parking, Charging, Routing

Wi-Fi Kiosks



Smart Streets: Light posts Monitoring Pollution, Noise, Traffic

Can We Trust Smart Cities?

- So many definitions of Trust….
  - "… the competence of an entity to act dependably, securely and reliably within a specified context."
  - "…the extent to which one party is willing to depend on somebody, or something, in a given situation … even though negative consequences are possible."
  - "Trustworthiness is the demonstrable likelihood that the system performs according to designed behavior under any set of conditions as evidenced by characteristics including, … security, privacy, reliability, safety and resilience." - NIST

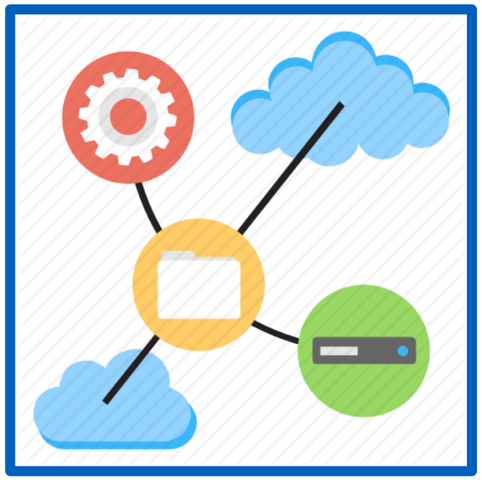
- Risk and trust have an inverse relationship

The lower the risk associated with the city, the more we can trust it!

Smart City Risk Factors

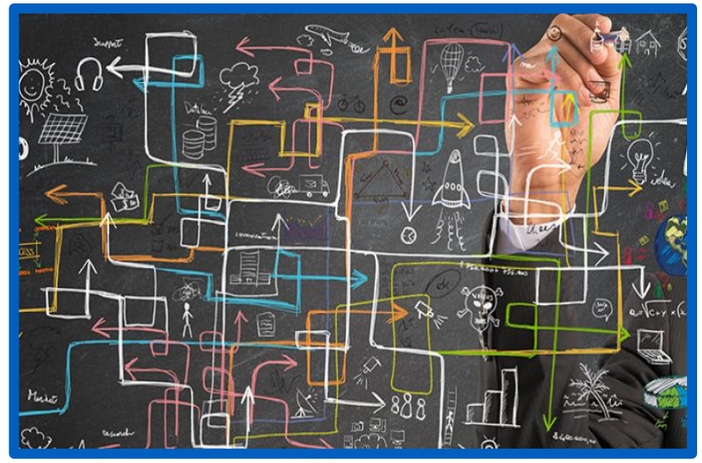
Non-Technical: aspects where humans are involved

- Management
- Training & education
- Governance and security practices



Technical: aspects where technology is involved

- Software development
- Devices and data
- Cyber attacks

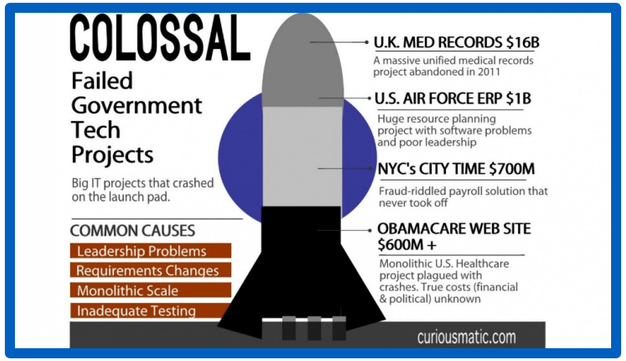


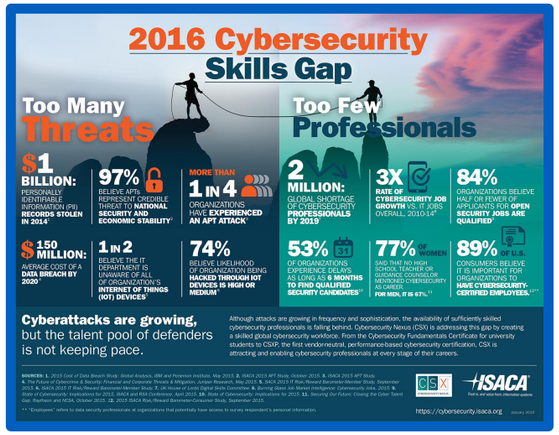
Complexity: a city is a complex multi-dimensional interconnection of human and technology systems

- Cascade effects
- Normal accident theory

Risk Factor: Non-Technical

Smart cities represent a fundamental change to the way that services are delivered, focusing on processes and people - how to make a city smart and who manages it





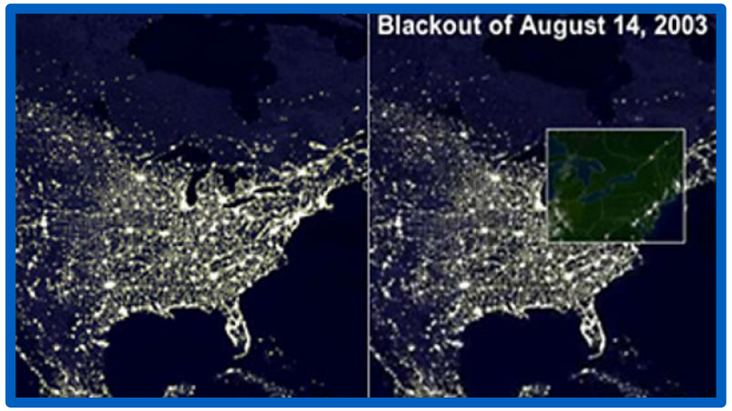
1. Management
   - Performance depends on effective management of the systems and infrastructure
   - IT deployment is complex - 85% of all IT projects fail due to non-technical aspects of innovation

2. Training and Education
   - Shortfall of as many as 1.5 million security experts by 2020
   - Shortage worse in public sector
   - Preventable human errors account for a large number of data breaches

3. Best Practices
   - Hardware and software released without security, and governments release it without testing
   - 200,000 vulnerable and insecure traffic control sensors were discovered in cities such as Washington D.C., New York, Seattle, San Francisco and London

Risk Factor: Technical

Technology is the enabler of a smart city, which includes hardware, software and cyber physical systems



1. Software Development
   - "We don't know how to write software without bugs. We've been trying for 70 years." – Vint Cerf
   - In a city running 100's of systems for critical services, a software bug in the alarm system had huge impact due to a chain reaction of events
   - Affected almost 10M people in Ontario, Canada and 45M people in 8 U.S. states


mirror.co.uk

WEDNESDAY 23.09.2015 DAILY MIRROR

Emission creep

» Millions of UK cars may be 'diesel exhaust cheats'

» VW boss 'loses vote of shareholders' confidence'

£10m boost for Mandarin in UK schools

Brits in shock over Algarve raider death

VOLKSWAGEN SHARE PRICE PLUMMETS

€106 ▼ 18.82%

"There is potential for this to spread to other car makers"

TAKING THE PISTON VW admit engine cheat

2. Trusting Data and Devices
   - Sensors can be hacked and fed fake data
   - Devices may misrepresent themselves - intentionally programmed to cheat
   - Delegating more control and decision making to devices can create more temptation to cheat
   - VW programmed its software to cheat on emissions tests
   - Growing need to validate, regulate and trust IoT devices

Risk Factor: Technical

3. Cyber Attacks

- Attack surface for smart cities is huge: wireless sensors will control everything from traffic lights to water management
- 2013 Symantec Security Threat Report: 22% of attacks are aimed at governments and energy/utilities companies; 24% of identity breaches are governments and healthcare institutions

2012 Hackers breached Canadian software company

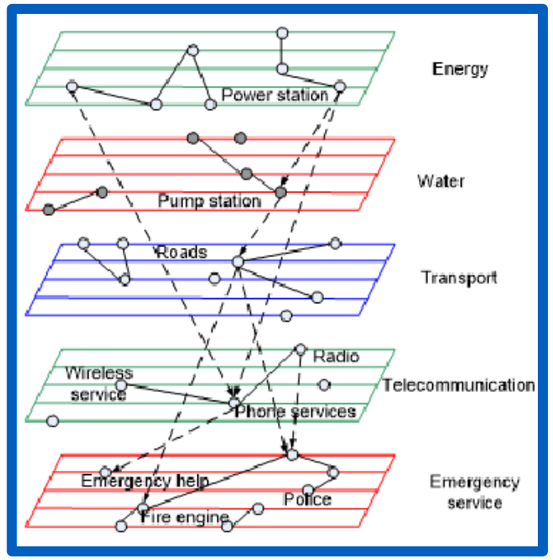
2014 Researchers black out city using smart meters

2015 Hackers remotely kill a Jeep on the highway

2018 City of Atlanta Ransomware attack

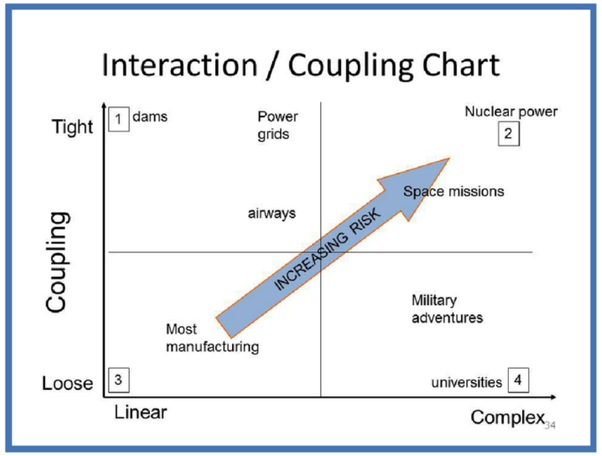
Risk Factor: Complexity

Smart cities are not discrete – they are complex multi-dimensional interconnection of diverse systems that promise unique services and optimum performance



1. Cascade Effects
   - City systems for critical services are interdependent - a bug or attack can cause chain reactions
   - What would commuting look like with non-functional traffic systems, no streetlights, and no public transportation?

2. Normal Accident Theory
   - Framework for characterizing complex systems according to risk
     - Ex: Air traffic, Chemical plants, Dams, Nuclear power
   - Accidents are presumed unavoidable because seemingly unrelated events accumulate to create major malfunctions
   - Three conditions make a system susceptible:
     - the system is complex
     - the system is tightly coupled
     - the system has catastrophic potential



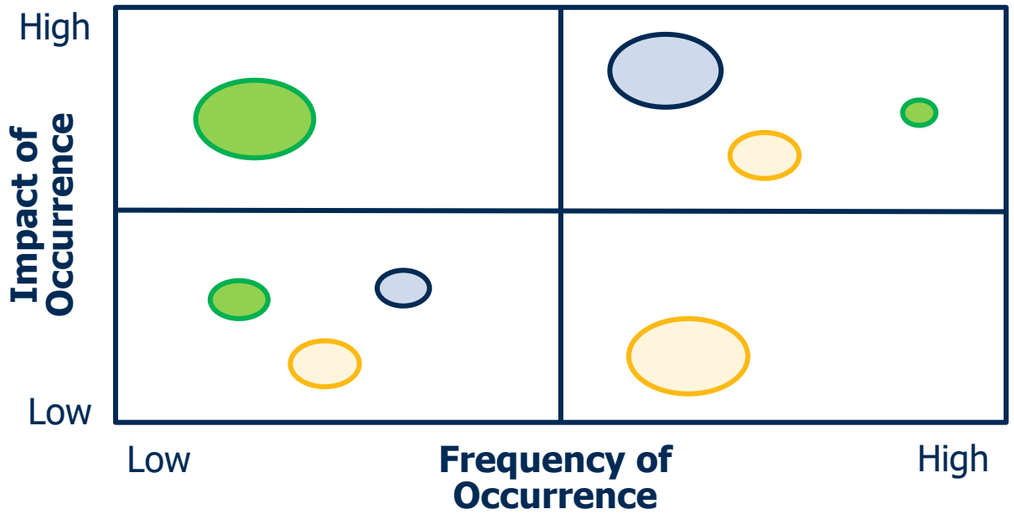
Evaluating the Trustworthiness of Cities

- Group threats into four categories
  - Imminent (current)
  - Not persistent (sometime)
  - Can recover from (tolerable)
  - Black swan (intolerable)

	Threat (current)	Threat (sometime)	Threat (tolerable)	Threat (intolerable)
Non-Technical	Risk Score	Risk Score	Risk Score	Risk Score
Technical	Risk Score	Risk Score	Risk Score	Risk Score
Complex Systems	Risk Score	Risk Score	Risk Score	Risk Score

- Grade how well a City can respond to the threats
  - Risk Score (low risk = high trust)

- How prepared are Cities for threats?
  - Frequency: not persistent to imminent
  - Impact: recoverable to black swan



Are We Overplaying the Cyber Risk to Cities?

"…the IoT links individuals' daily lives to that of the internet. This interconnectedness between people and cyberspace gives criminals, extremists, and adversary nation-states a vector to target individuals, private and governmental organizations, and U.S. civil society as a whole, and, in the process, it has inspired a fear of the unknown. In short, **cyber is the new weapon of mass destruction threat**, and addressing it will require marshalling the resources of the entire interagency."

U.S. Army Major Quan Hai T. Lu, Deputy Chief of Systems Vulnerability & Assessment at the Defense Threat Reduction Agency

2015

The US Must Prepare for a Cyber 'Day After'

- During the height of the Cold War, the U.S. had plans for the "day after" a massive nuclear strike:
  - How to assure continuity of the government
  - How to get transportation and communications back online
  - How to put hard currency back into circulation and begin regenerating the economy
- U.S. government has warned that foreign nations have been hacking our critical infrastructure and inserting malware that could sabotage dams, pipelines, water supplies, or even transportation systems
  - We currently have no reconstitution plans for a cataclysmic cyber event
- Continuity of the Economy, or COTE, plan
  - Ensure that critical data and technology would be available to get the economy back up and running after a catastrophic cyberattack
  - Planners must figure out what "seed data" would need to be preserved in a protected and verified format, with a process to assure no corruption or manipulation

Defense One website, 28 August 2019

Conclusions

- Combination, connection and integration of systems and infrastructures are fundamental to a city being smart
  - Greater possibility that things can go wrong
  - More vulnerable it is to different types of risk
- Technology alone won’t solve trust problems
  - Technology: change and upgrade technological tools to improve services and create conditions where the tools can be better used
  - Organization: managerial and organizational capabilities for effective use of technological tools and conditions for their use
  - Policy: address institutional and non-technical urban problems and create conditions that enable a smart city
- Need a holistic approach to trusting smart cities. to overcome the adverse impact of siloed organizational structures